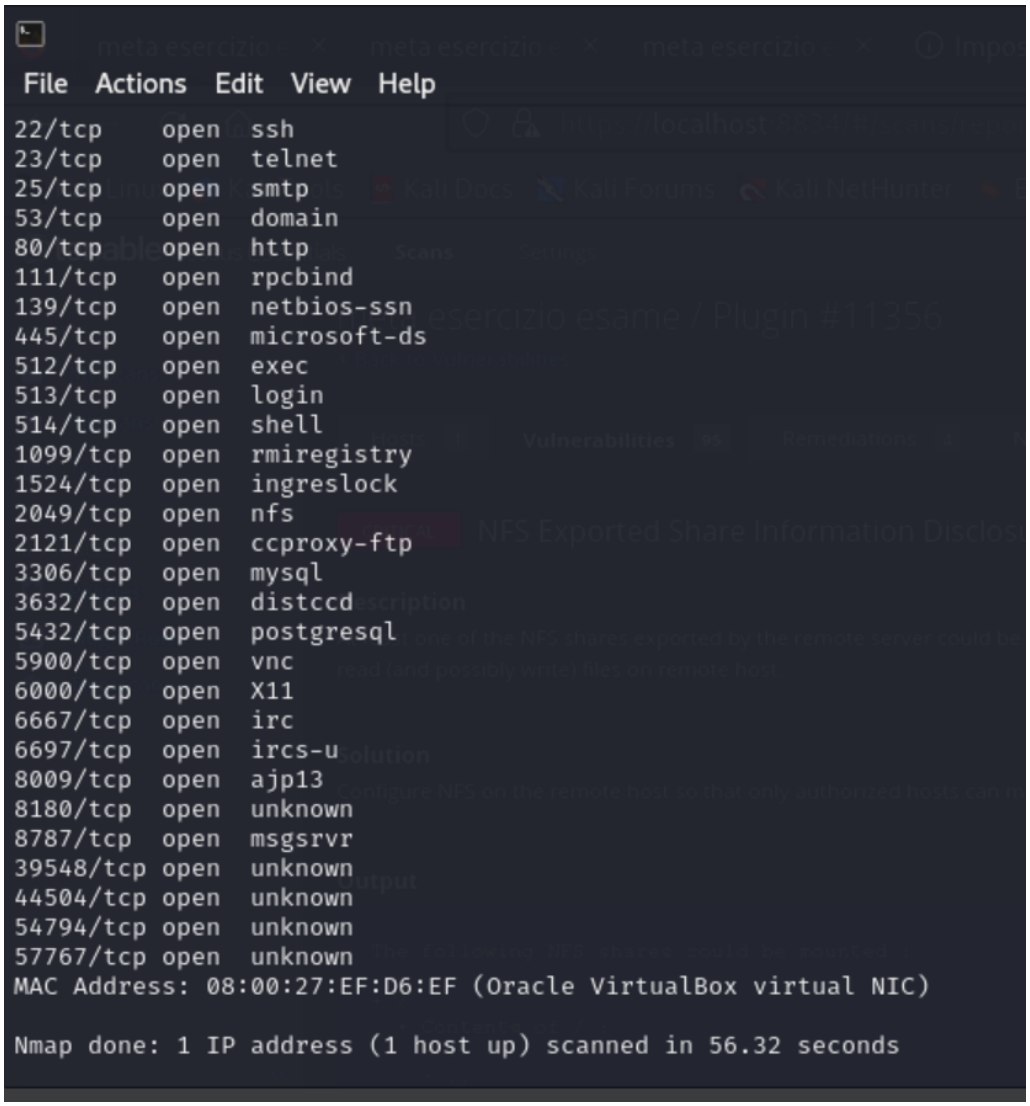
W12D4

BIND SHELL BACKDOOR DETECTION:

Per prima cosa ho aperto kali, usando netcat per connettermi alla porta 1524.



Una volta trovata la porta (nella quale era già riportata nella scansione con Nessus)

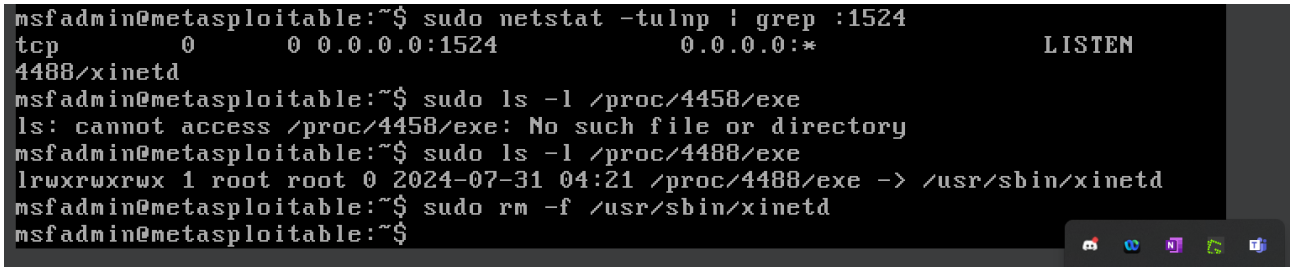
Ho usato il comando: SUDO NETSTAT -TULNP | GREP su Metasploitable per trovare quale processo sta ascoltando su quella porta.

IL PID DEL PROCESSO è 4488.

POI CON SUDO LS -L /PROC/4488/EXE HO TROVATO LA PATH DEL FILE.

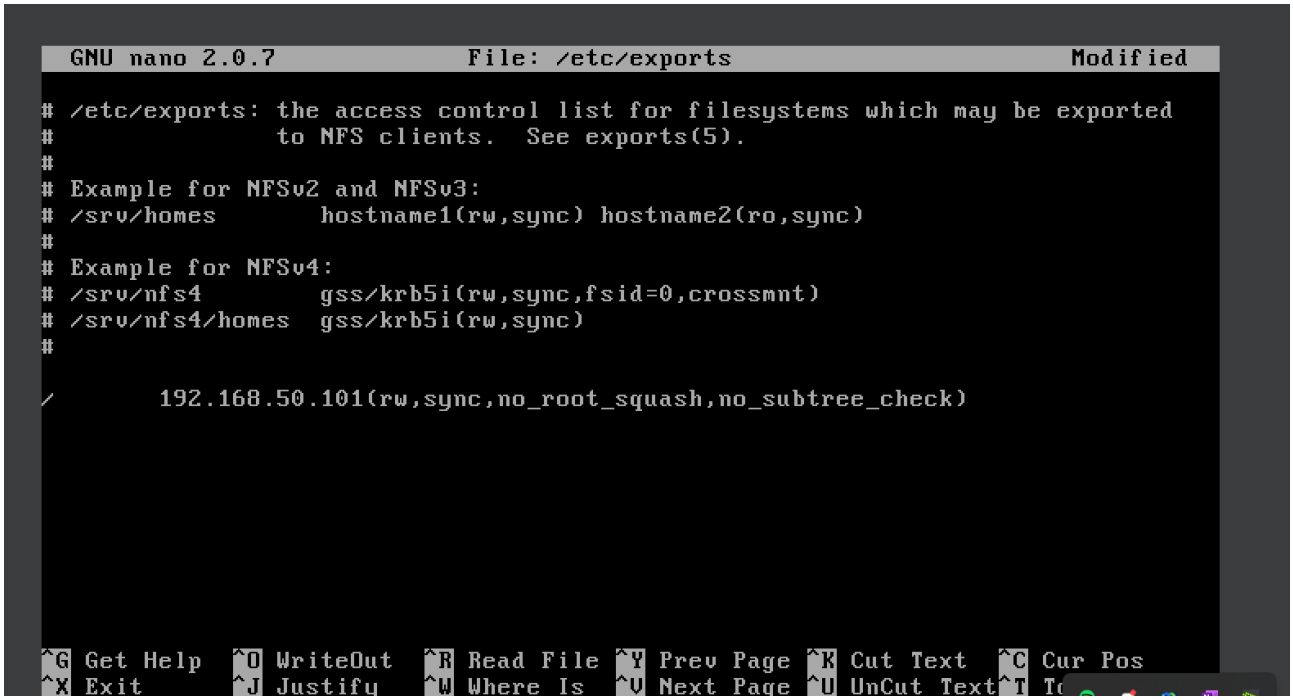
INFINE CON IL COMANDO SUDO RM -F /USR/SBIN/XINETD HO RIMOSSO IL FILE COME IN FIGURA.

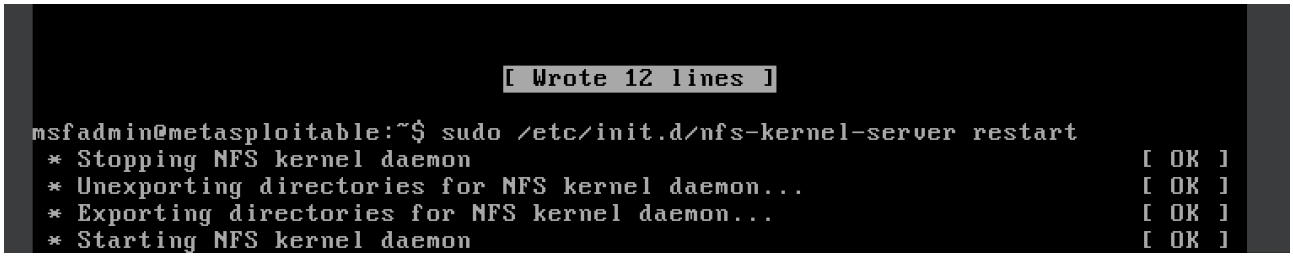
Alla fine ho fatto sudo nano /etc/rc.local per commentare le righe senza gli #



NFS EXPORTED SHARE INFORMATION DISCLOSURE

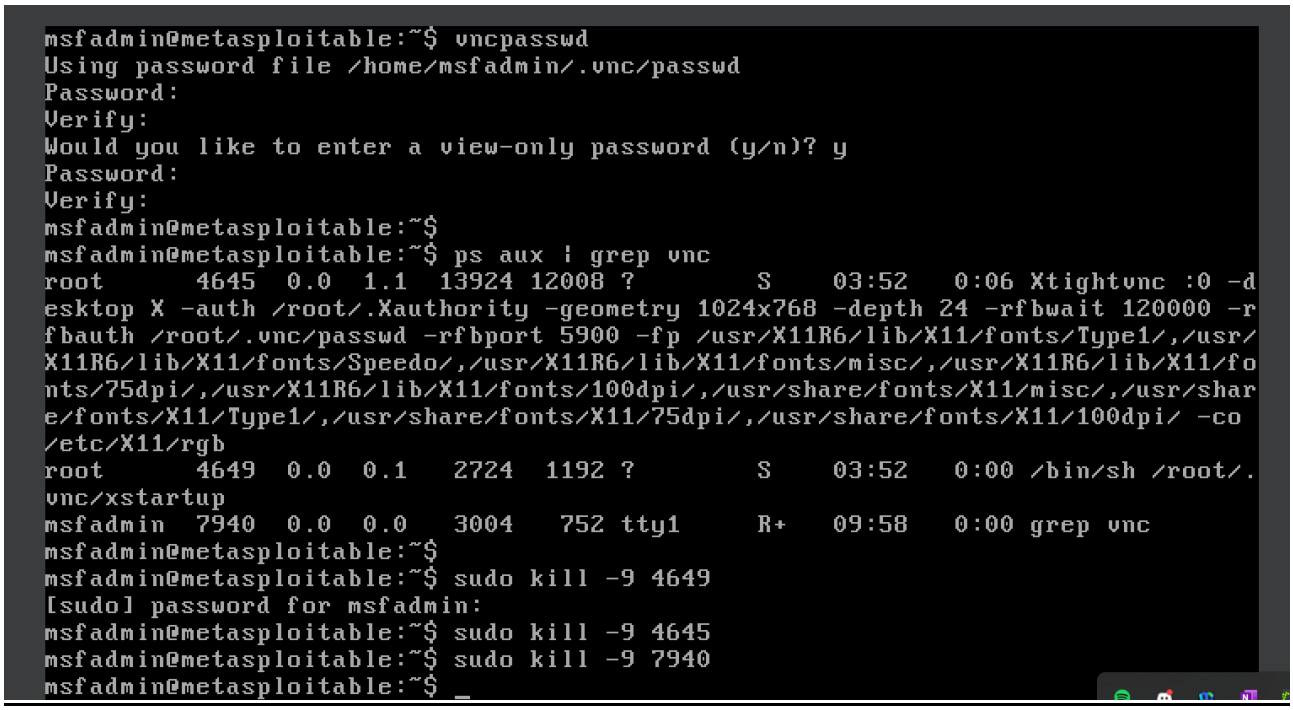
Per rimuovere questa vulnerabilità è stato necessario rimuovere l' asterisco che permetteva l' accesso a qualsiasi host.





Alle fine ho lanciato il comando: sudo /etc/init.d/nfs-kernel-server restart

VNC SERVER PASSWORD



Per rimuovere tutte le vulnerabilità ho rimosso tutti i processi con la vecchia password.

In seguito, ho creato una nuova password con il comando vncpasswd, e fatto ripartire il server con il comando vncserver:1

Per avere conferma della password cambiata, ho usato il comando: sudo ls -l /.vnc/passwd